#654 6/11/09

1663 Mission Street
Suite 602
San Francisco
California 94103

t 415.255.9499
f 415.255.9792
e ilrc@ilrc.org
w ilrc.org

April 10, 2009

Office of Consumer Affairs and Business Regulation
Ten Park Plaza, Suite 5170
Boston, MA 02116
Phone: (617) 973-8700
Fax: (617) 973-8799

Office of Attorney General Martha Coakley
One Ashburton Place
Boston, MA 02108
Phone: (617) 727-2200

Delivery Via UPS Tracking No. 1Z2679200396299156 and 1Z2679200396679361

RE: Notification of Data Security Breach Incident

Dear Sir/Madame:

This letter is being sent in accordance with state law to inform your office that our company recently discovered that certain information about approximately 340 individuals was taken by an unauthorized computer intrusion into one of our databases and may have been misused. The information included name and credit card number. We have enclosed a copy of the notice letter that we will be sending to affected individuals in Massachusetts on April 10, 2009.

We have not notified the three Consumer Reporting Agencies of this incident. The incident was brought to our attention on February 6, 2009. Immediately upon discovery of this incident we conducted an investigation and filed a resolution claim with the internet search service demanding that all sensitive information pertaining to our customers be immediately removed. This was accomplished by February 17, 2009. We have conducted tests and have confirmed the removal of our customer information. We have submitted our website to a security audit, and we are implementing a new ecommerce system to prevent future incidents such as this.

Should you have any additional questions, you may contact me directly at 415-255-9499 x587.

Sincerely,

Shari Kurita
Assistant Director
Immigrant Legal Resource Center

Enclosures

RECEIVED
APR 21 2009
OFFICE OF CONSUMER AFFAIRS

1663 Mission Street
Suite 602
San Francisco
California 94103

t 415.255.9499
f 415.255.9792
e ilrc@ilrc.org
w ilrc.org

April 10, 2009

Dear ILRC seminar and webinar registrants,

On about February 6, 2009 we discovered that your personal information may have been exposed or misused. Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident; however no police report has been filed. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may need to give copies of the police report to creditors to clear up your records.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. If you are a victim of identity theft you also have the right to obtain a police report. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348 (www.equifax.com); Experian Security Freeze, P.O. Box 9554, Allen, TX 75013 (www.experian.com); and TransUnion Security Freeze Fraud Victim Assistance Department, P.O. Box 6790, Fullerton, CA 92834 (www.transunion.com) by regular, certified or overnight mail.

In order to request a security freeze, you will need to provide the following information: (1) Your full name (including middle initial as well as Jr., Sr., II, III, etc.); (2) Social Security Number; (3) Date of birth; (4) If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years; (5) Proof of current address such as a current utility bill or telephone bill; (6) A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); (7) If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft; (8) If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit bureaus must send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to place, lift or remove the security freeze.

On behalf of our Board and Staff, I want to reassure you and emphasize we have not taken this breach lightly. The process of securing data and ensuring content integrity has been reviewed. Additional security steps and documentation are being put in place to prevent such a release from happening again. We deeply regret any inconvenience this may cause. Please do not hesitate to contact me directly at (415) 255-9499 x587 with your concerns or questions. Thank you for your understanding and support.

Sincerely,

Shari Kurita
Assistant Director
Immigrant Legal Resource Center

Immigrant Legal Resource Center
Security Breach FAQ's
March, 2009

Q1: What is this about?
A1: On February 6, 2009 the ILRC discovered a breach in our website's ecommerce security involving customers' names and credit card numbers for customers who registered for seminars during November 2007 through December 2008. Our investigation indicates that sometime in January 2009 a web search engine breached our website security and cached this sensitive information.

Q2: What is ILRC doing?
A2: We immediately conducted an investigation and filed a resolution claim with the internet search service demanding that all sensitive information pertaining to our customers be immediately removed. This was accomplished by February 17, 2009. We have conducted tests and have confirmed the removal of our customer information. We have not taken this incident lightly; we have submitted our website to a security audit, and we are implementing a new ecommerce system through Paypal.

As a precaution, ILRC is providing notification to people who registered for seminars through our website during the period November 2007 through December 2008 so that if it turns out the information was compromised in any way, they can take appropriate action to protect themselves. We have been investigating the incident and this investigation is continuing.

Q3: What information was involved?
A3: The information that the web search engine cached included name, address and credit card numbers of people who registered for our seminars through our website between November 2007 and December 2008.

Q4: Were Social Security Numbers exposed?
A4: No.

Q5: Were credit card numbers exposed?
A5: Yes.

Q6: Were bank account numbers exposed?
A6: No.

Q7: Were drivers license numbers exposed?
A7: No.

Q8: If my information was involved, what should I do?
A8: If you received a letter from ILRC then your information was potentially involved. This includes the credit card account number that you used to register for our seminar. You should contact one of the three credit reporting bureaus and place a 90-day Initial Fraud Alert on your credit file. That bureau will notify the other two bureaus and will send you confirmation that the alert has been placed along with a free copy of your credit report. Review your credit report carefully to see if there has been any new credit requested.

Also review your account statements carefully to see if there have been any charges that you have not authorized. If there are, contact your Bank or card issuer immediately at the number on your monthly statement. Even if there has been no unusual activity on your account, you can ask your bank to change your account number. Mark on your calendar to review all this information again every three months. Sometimes identity thieves will wait for time to pass before using your information.

Q9: How will I know if my information was used by someone else?
A9: The best way to find out is to carefully review your credit card statements to look for unauthorized activity and to get a copy of your credit report from one of the three credit reporting bureaus. The credit report will show if

there has been any new credit requested using your information.

You should check your account statements carefully. If someone else has used your credit card number the activity will appear on your statement. If you see activity that you did not authorize, call your bank or card issuer at the number on the back of your statement immediately and tell them that the activity was not authorized and ask the bank to change your account number.

Q10: Should I change my credit card number?
A10: You should review your account activity carefully. Even if you do not find any unusual activity, you may want to contact your credit card issuer immediately and request a change of account number as a precaution.

Q11: How do I put a Fraud Alert on my credit report?
A11: US law allows you to put a "fraud alert" on your credit report. This is a free service. A 90-day Initial Fraud Alert puts a statement on your credit file that you may have been or are about to become the victim of identity theft or other fraud. If you specify a telephone number, anyone using your credit report must call that number or take reasonable steps to verify your identity to confirm that a credit application is not the result of identity theft.

After you put a fraud alert on your credit report, you will be asked to provide proof of your identification when you apply for credit. This may limit your ability to apply for instant credit for in-store purchases but it should not interfere with your daily use of existing credit cards or banking accounts.

You can put a 90-day Initial Alert on your credit report by contacting one of the three major credit bureaus. The one you contact will notify the others. This will entitle you to a free credit report. You will receive confirmation of the alert from the bureau you contact. At the end of the 90 day period you may place an additional Initial Fraud Alert on your credit file. We suggest that you do this every 90 days for at least one year.

Q12: How can I get in touch with the credit bureaus?
A12: There are three major credit bureaus. They are:

Experian:	Equifax:	Trans Union
888-397-3742	800-525-6285	800-680-7289
P.O. Box 2002	P.O. Box 740241	Fraud Victim Assistance Division
Allen, TX 75013	Atlanta, GA 30374-0241	P.O. Box 6790
		Fullerton, CA 92834-6790

Q13: Do I have to pay for a credit report?
A13: You are entitled to one free credit report a year from each of the three credit reporting bureaus. This means that you can receive one today from one (e.g. Experian), you can receive another in four months (e.g. from Equifax), and you can receive another in eight months (e.g. from TransUnion). By spacing out your requests for your free credit report you can monitor your credit over the course of a year. If you want to receive more than one credit report form any of the credit reporting bureaus during the same year, you may have to pay a small charge.

Q14: How long will it take to get my credit report?
A14: You can access your credit report online at www.annualcreditreport.com. You can download or print the report from that site. You may also request the report by telephone (by calling 1-877-322-8228 and answering some questions to verify who you are) or by mail (by downloading the request form from www.annualcreditreport.com and mailing it to **Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281).** If you request your report by phone or by mail it will take approximately two weeks to process the request, so you should allow two to three weeks for delivery to you.

Q15: What is a fraud alert?
A15: A fraud alert is a message added to your credit report that tells anyone who pulls a copy of your credit report telling them that there is possible fraud associated with your account. It gives them a telephone number to call you before issuing any new credit.

A 90-day Initial Fraud Alert expires after 90 days. If you have been the victim of identity theft you may be able to place a 7-year fraud alert on your account. You can obtain more information online at http://www.consumer.gov/idtheft.

Q16: How long does a fraud alert last?
A16: The Initial Fraud Alert lasts 90 days after it is placed on your report. You can remove the alert by calling the credit bureaus before the 90 days expires. You can place an initial alert every 90 days by calling one of the credit bureaus.

Q17: Will a fraud alert stop me from using my credit cards?
A17: No. However, a fraud alert may interfere with your ability to get immediate credit, for instance if you apply for instant credit at a department store. This is because the department store credit office will have to call you to verify your identity before issuing you credit.

Q18: Can I still apply for credit if I put a fraud alert on my credit report?
A18: Yes. The fraud alert may slow down the process of getting approval for credit because the fraud alert will require that the creditor verify your identity before approving new credit.

Q19: What should I watch out for on my credit report?
A19: Look for any accounts that you don't recognize especially new accounts. Look in the personal information section to see if the residence and employment information is correct or has changed.

These things could be indications of fraud. If you see information you do not understand or that is wrong, call the credit bureau at the number on the report and speak to a staff member. If the information cannot be explained, contact your local police or sheriff's office.

Q20: If someone has used my information, what should I do?
A20: You should immediately notify your local police or sheriff's office and file a report. Get a copy of the police report, because you may need to give a copy to the credit bureaus or creditors. Also contact one of the three credit bureaus and place a fraud alert on your account. For more information you can visit the website: www.consumer.gov/idtheft

Q21: Do I have to call all three credit bureaus?
A21: When you call one bureau, it will pass the report on to the other two. You should receive a confirming letter from each of the three bureaus. If you do not receive confirmations from all three credit bureaus, call the bureau which did not confirm the alert.

Q22: Will ILRC contact me to ask for my personal information because of this event?
A22: No. We will not contact you unless you call or write to us first. We will never ask for bank account information or personal identification numbers (PINs) or for your full credit card or social security number. If you are contacted directly by someone who claims to be with ILRC and who ASKS YOU FOR YOUR PERSONAL INFORMATION, please **immediately** contact us and your local sheriff's office to report the suspicious contact.

Q23: I have been contacted directly by someone claiming to be from ILRC or a law enforcement agency asking for my personal information (e.g., social security number, etc.). Did you contact me? What should I do?
A23: No. We did not contact you unless you called or wrote us first. We would never have asked for bank account information or personal identification numbers (PINs) or for your full credit card or social security number. If you were contacted directly by someone who claimed to be with ILRC or law enforcement and who ASKS YOU FOR YOUR PERSONAL INFORMATION, please **immediately** contact us and your local sheriff's office to report the suspicious contact. You may also provide us with your name and telephone number and we will have the appropriate authorities contact you directly. When law enforcement contacts you, they will reference your contact with ILRC.

REFERENCE SHEET FOR WEBSITES:

Credit Reporting Bureaus:

Annual Credit Reports:
http://www.annualcreditreport.com

Experian:
888-397-3742
P.O. Box 2002
Allen, TX 75013
http://www.experian.com

Equifax:
800-525-6285
P.O. Box 740241
Atlanta, GA 30374-0241
http://www.equifax.com

Trans Union:
800-680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
http://www.transunion.com

Federal Trade Commission

Identity Theft
Hotline: 877-ID-THEFT (877-438-4338)
http://www.consumer.gov/idtheft
Affidavit: http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf

Filing a Complaint with the FTC
http://www.ftc.gov
1-877-FTC-HELP (1-877-382-4357) (TTY: 1-866-653-4261)

Social Security Administration

Fraud Hotline: 800-269-0271
Benefits Statement: 800-772-1213
http://www.ssa.gov

Privacy Rights Clearing House Identity Theft Resources

http://www.privacyrights.org/identity.htm
This not-for-profit organization provides statistics, fact sheets and government records about identity theft.

Identity Theft Resource Center

http://www.idtheftcenter.org
This not-for-profit organization is dedicated exclusively to identity theft. It provides consumer and victim support about identity theft and includes resources, consumer alerts and instructions for victims.